AI: Leveling the Cybersecurity Playing Field

SECURITY BOULEVARD

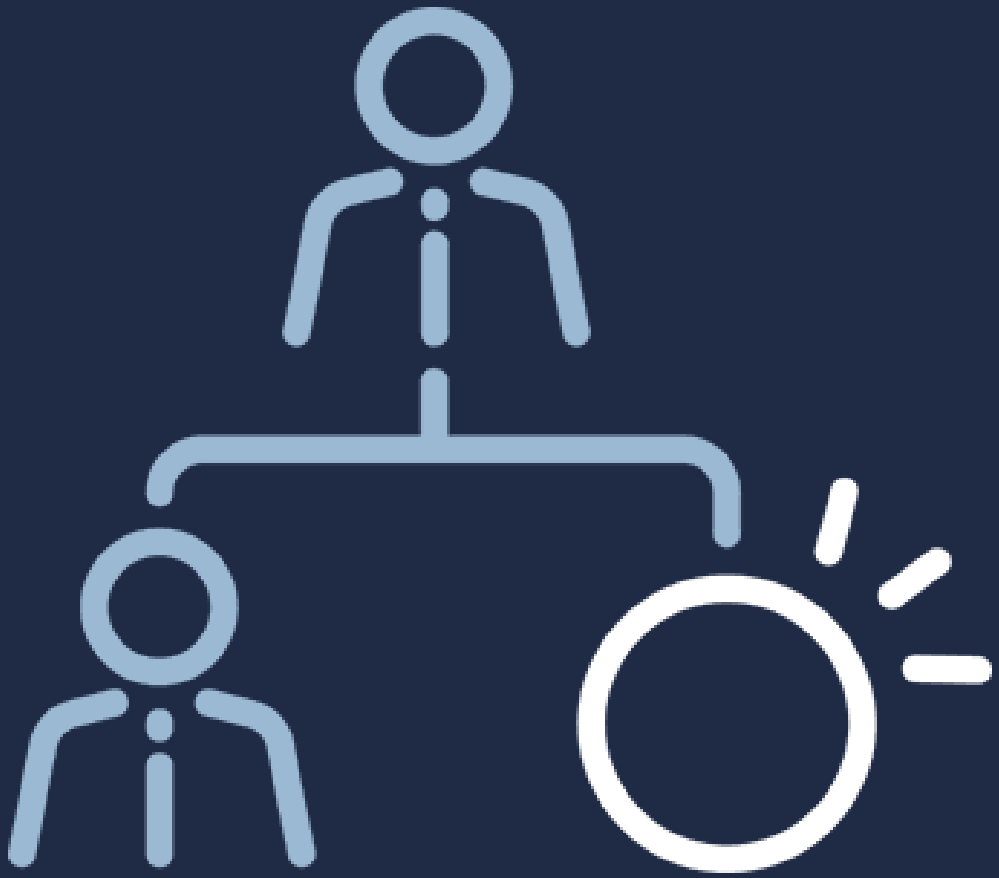
The increase in volume and sophistication of cyberattacks has left cybersecurity teams overwhelmed. There isn't enough natural intelligence available to combat cyberattacks that victimize organizations large and small.

The only way to level the playing field is to augment cybersecurity teams with the artificial intelligence (AI) required to detect attacks sooner and more accurately and respond faster. AI isn't likely to ever replace the unique ability of humans to identify new types of attacks and vulnerabilities, but they will eliminate mundane tasks and reduce the alert noise that prevents attacks from being recognized until it's too late.

Cybersecurity AI platforms may still have a lot to learn about the IT environments they protect. However, just like humans, the more they learn the better they become. The only difference is cybersecurity AI platforms never quit, take a day off, or forget something once they learn it.

Drivers of Cybersecurity AI Investments

Following a 6.4% increase in 2020, worldwide spending on information security and risk management technology and services is forecast to **grow 12.4%** to reach **$150.4 billion** in 2021.[1]



The global shortage of cybersecurity personnel today stands at **3.12 million**.[2]

The Promise of Cybersecurity AI

The Promise of Cybersecurity AI

Two-thirds of organizations believe AI will help identify critical threats.

Three-quarters said AI allows their organization to respond faster to breaches.

Three in five firms said AI improves the accuracy and efficiency of cyber analysts.[3]

Fear and Loathing of Cybersecurity AI Declines

43% of companies use AI and machine learning technologies.[4]

The cybersecurity AI market is projected to reach **$38.2 billion** by 2026, a 23.3 compound growth rate from 2019.[5]

Other Considerations

Build Versus Buy

IT teams can build and train AI models to analyze cybersecurity threats if they have enough data. The cost of maintaining those AI models, however, may be cost-prohibitive compared to a cloud service.

Transparency Is Crucial

Organizations that employ AI platforms need to be able to be able to explain how it works.

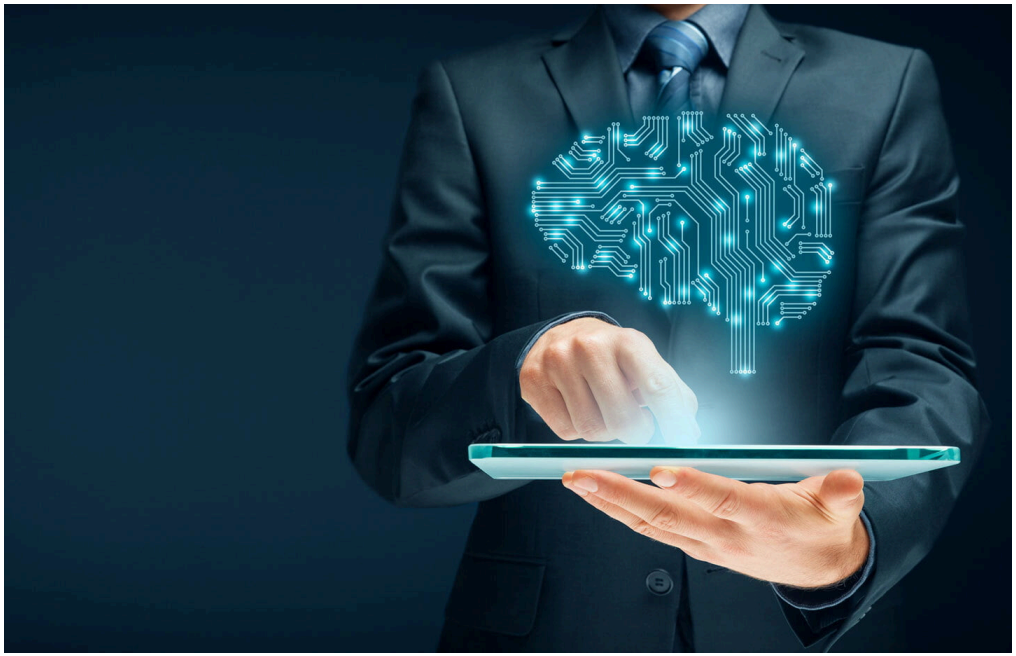
Cybercriminals Will Employ AI

Machine learning algorithms will make it easier to scan for vulnerabilities at scale faster.[6]

Deepfakes are being used to launch sophisticated phishing attacks to compromise credentials.[7]

Cybersecurity AI Augments, Not Replaces, Security Professionals

AI is only as good as the model it's built on. No matter how advanced AI becomes, identifying new types of cyberattacks will always be difficult.[8]



Thank you for reading

AI: Leveling the Cybersecurity Playing Field